UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/099,735	03/15/2002	James H. Price	1348-1013	4217

32376 7590 07/19/2006

LAWRENCE R. YOUST
DANAMRAJ & YOUST, P.C.
5910 NORTH CENTRAL EXPRESSWAY
SUITE 1450
DALLAS, TX 75206

EXAMINER	
GEE, JASON KAI YIN	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 07/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/099,735	PRICE ET AL.	
	Examiner	Art Unit	
	Jason K. Gee	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to communication: amendment filed on 06/01/2006.

2. Claims 1-18 are currently pending in this application. Claims 1, 10, and 15 are independent claims.

3. No IDS was received for this application.

Specification

4. In view of Applicants' amendment, the previous objections to the Specification are withdrawn.

Claim Rejections - 35 USC § 112

5. In view of Applicants' amendment, the previous 112 rejections are withdrawn.

Response to Arguments

6. Applicant's arguments filed 06/01/2006 have been fully considered but they are not persuasive.

7. As per claim 15, the applicant argues that the Jerdonek reference does not teach the 'means-plus-function' as taught in the applicants specification. However, Jerdonek does indeed teach all the further limitations of the 'means-plus-function' found in the applicants specification. As seen in the applicants specification for example, the applicants claims a means for receiving a new user key set. From the specification, the

applicants teach that means for receiving a new user key set is hardware in a client device. Jerdonek teaches in paragraph 48 that a new user key set is received by a client device.

Also, as per claim 15, the applicants have added the further limitation of "means for conducting a registration session with a registration server." However, Jerdonek still teaches this, in paragraph 46, in which an authentication server connects with an external server and communicates with each other. This communication is a registration session, and the means for this communication is via the Internet, as taught in paragraph 45 and shown in Figure 1.

8. As per claims 1-14 and 16-18, the applicants argue that Jerdonek fails to teach other limitations recited within the pending claims, including, but not limited to the three-step, two server authentication process recited in claims 1 and 10. However, the applicants does not explicitly teach two servers.

Also, the applicants argue that Jerdonek teaches an external server to the network, whereas the applicants cite that the equivalent 'authenticator' is "in" the network. Jerdonek does indeed teach an external server which is equivalent to the authenticator. However, as can be seen in Figure 1, Jerdonek is an external server, but it is still included within the network, as it is part of the computer network 160.

Furthermore, the applicants argue that the Stallings reference does not disclose elements such as 'common key set' and a 'new user key set,' or separate authentication and registration servers ' as recited in the pending claims. First of all, the applicants never claim an authentication server. Secondly, the Examiner is not using the Stallings

reference to reject the common key set and the new user key set. This is already rejected using Jerdonek. Stallings is used as a reference to teach that an authenticator can determine whether keys are valid. As seen in the rejection, Jerdonek does indeed teach SSL, but does not mention the specific details regarding it. The Examiner uses the Stallings reference to teach the specifics of SSL, which is inherent to the protocol, to clarify that Jerdonek does teach wherein an authenticator may determine if keys are valid. The Stallings reference shows that an authenticator does determine when a key set is valid in the SSL protocol, and thus, Jerdonek teaches this limitation, as Jerdonek teaches SSL. The applicants also argue that the Stallings reference fails to teach additional limitations, including the step of providing the client system with limited network access after authentication of the common key set. However, as stated before, Stallings was not used to teach this, as Jerdonek already teaches this, as described in the rejection (as stated in Jerdonek paragraphs 45-46, where a client may access only a registration server).

9. As per claims 9, 12, and 16-18, the applicants claim that the Ketcham references does not teach the limitations that the Jerdonek and Stallings reference does not explicitly teach. The Ketcham reference is applied to the limitation that the client device authenticates a userkey set by determining if the key is received from a valid source. As taught in the art rejections below, Ketcham does teach this. Col. 10 lines 10-25, where it cites "Remote terminal 102, however, has not verified network 108 as being authentic. To facilitate this bidirectional process, network server 108 generates a mobile authentication response. Mobile authentication response 534 is comprised of

the authentication response 530 as received from remote terminal 102 yet further encrypted by 108. In an alternative embodiment, network server 108 (Figure 3) retrieves mobile authentication response 306 (Figure 3) for transmission to remote terminal 102. Such an encrypted response when received by remote terminal 102 demonstrates the authenticity of network server 108." As seen in this passage, it is clear that the client device authenticates by determining if something is received from a valid source. As seen in the arguments above, the Jerdonek and the Stallings reference teaches all the limitations found in the independent claims.

10. As per claim 11, the applicants argue that the Walker reference does not teach the further limitations of claim 11. However, the Walker reference does indeed teach the further limitations of this claim, as seen in the art rejection below. As stated in the rejection, Walker is used to reject the further limitation of an authentication database that associates a plurality of common key sets with a plurality of registration servers, as seen in paragraph 17. As seen in the arguments above, the Jerdonek and the Stallings reference teaches all the limitations found in the independent claims, and Walker is used to reject the further limitations of the dependent claim.

11. As per claims 13-14 and 17-18, the applicants argue that the Heller reference does not explicitly teach the further limitations of these claims. The applicants have recited though "The Examiner has not asserted that **Walker** cures the above-recited deficiencies of Jerdonek and Stallings...". The Examiner believes that the applicants are actually referring to Heller, as this is found under the section in which the applicants are arguing about the Heller reference, and not the Walker reference. The Walker

reference is not even used for these claims. Therefore, the Examiner will proceed to read the arguments as applied to the Heller reference, and not the Walker reference. As the applicants argue that the Heller reference does not teach the further limitations of claims 13-14 and 1718, the Examiner asserts that Heller does indeed teach these limitations. Heller is applied to teach the use of PPP, as the references recited earlier (Stallings and Jerdonek) already teaches signaling the authenticator and registration server. As well known in the art, PPP is a common communication service. The Heller reference is used an example to show that PPP may be used to communicate. As taught in the art rejection seen below, Heller teaches the use of PPP to communicate in paragraphs 19 and 20. As seen in the arguments above, the Jerdonek and the Stallings reference teaches all the limitations found in the independent claims.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Independent claim 15 is rejected under 35 U.S.C. 102(e) as being anticipated by Jerdonek US Patent Application Publication 2002/0095569 (hereinafter '569).

As per independent claim 15, '569 teaches a client device ('key wallet' paragraphs 39-40) installed I a data network access device (client systems, Figure 1, systems 130, 140, 150). Routers are taught in paragraph 23 and the IP protocol is sued, as indicated in paragraph 26. The network access device includes the router, as Figure 1 and paragraph 23 display and describe the client devices connecting to the routers. The network devices as indicated in paragraph 26 can utilize the Internet Protocol, which indicates the system can route IP signals from different networks. The clients can connect to a network with a plurality of users connected to the network access device, as the clients can connect to a local area network or an intranet. Means for storing a preprogrammed common key set is taught in paragraph 39. Means for requesting access to the remote data network utilizing the preprogrammed common key set for authentication purposes when the client device is installed in the network access device is taught in paragraph 44. Means for receiving a new user key set from the network is taught in paragraphs 47-48. These paragraphs along with paragraphs 49-53 indicate that the common key set is replaced with the new key set, as the new key set is used to connect to the remote server. Means responsive to receiving the new user key set for automatically requesting access to the remote data network utilizing the new user key set for authentication purposes is also taught in paragraphs 47-48, and paragraph 61 teaches that it may be automatic. Also, means for conducting a registration session with a registration server are taught in paragraphs 46 and 47, in which a session is established via the Internet, in which registration processes occur.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerdonek ('569), and further in view of William Stallings' *Cryptography and Network Security – Principles and Practice*, Second Edition (1999).

As per independent claim 1, '569 teaches a method of automatically configuring and authenticating a client device('key wallet' paragraphs 39-40) installed in a data network access device (client systems, Figure 1, systems 130, 140, 150). Routers are taught in paragraph 23 and the IP protocol can be used, as indicated in paragraph 26. The network access device includes the router, as Figure 1 and paragraph 23 display and describe the client devices connecting to the routers. The network devices as indicated in paragraph 26 can utilize the Internet Protocol, which indicates the system can route IP signals from different networks. The clients can connect to a network with a plurality of users connected to the network access device, as the clients can connect to a local area network or an intranet. Paragraph 39 teaches that a user has a preprogrammed common key set. Requesting access to the remote data network by the client device using the preprogrammed common key set for authentication purposes

is taught in paragraph 44. Paragraph 45-46 then goes on to teach that the client is directed to a registration server (authentication server 350) after it is authenticated (the common key set is valid). The registration server is accessed, and the client receives a new user key set (paragraphs 47-48). Requesting access to the remote data network by the client device using the new user key set for authentication purposes is taught in paragraphs 49 and 50. The client device has then full network access upon determining that the new user key set is valid (paragraph 60). Paragraph 61 also teaches that all these steps may be automatic.

However, '569 does not explicitly teach that an authenticator can both determine whether the common key set is valid and also determining whether the new user key set is valid. In '569, the 'external server' 310 authenticates both the common key set and the new user key set. '569 teaches the use of an SSL connection from the client to the server in paragraph 45, but does not teach the specifics of it. The specifics of SSL can be taught by Stallings. With an SSL connection, a client and his key are authenticated by a server, as indicated on pages 454 and 455. In this way, the 'external server' in '569 is an authenticator of the common key set, as the client connects to this the external server using SSL. Also, the external server authenticates the second key set, as it receives the digital signature of the new key set through a secure communications line such as SSL described in '569 paragraphs 59-53.

At the time of the invention, it would have been obvious to combine '569 with Stallings to include that a server authenticates a client in an SSL connection. One of ordinary skill in the art would have been motivated to perform such an addition as

mutual authentication is a standard for SSL. The specifics of SSL can be found on pages 451 to page 455 of Stalling's book.

As per claim 2, the step of requesting access to the remote data network by the client device using the common key set for authentication purposes includes automatically requesting access to the remote data network by the client device using the common key set for authentication purposes (paragraph 61 of '569).

As per claim 3, paragraph 46 of '569 teaches that the registration server is associated with the common key set in an authentication database. Providing the client device with limited network access includes providing the client device with access only to a registration server is already rejected in claim 1. The registration server is associated with the common key set, as the registration server cannot be accessed until the common key set is used or accessed, as can be seen in the steps leading up to accessing the registration server.

As per claim 4, paragraph 61 of '569 indicates that the registration server can automatically assign the new user key set. Sending the new user key set from the registration server to the client device is already rejected in claim 1.

As per claim 5, paragraphs 47-48 of '569 teaches that a new user key is sent from the registration server (authentication server 350) to an authenticator (external server 310).

As per claim 6, paragraphs 47-48 of '569 teaches that a new user key set is sent from the authenticator to the client device. As rejected in claim 1, the authenticator is the external server.

As per claim 7, the user selects the new user key set as the user requests a key and obtains it from the authentication server 350, as described in '569 lines 45-48.

As per claim 8, paragraphs 47-48 of '569 teaches that the new user key is sent from the registration server (authentication server 350) to an authenticator (external server 310). These paragraphs also teach that the key is sent from the authenticator to the client device.

Independent claim 10 is rejected using the same basis of arguments used to reject claim 1, as claim 10 is directed to an apparatus. '569 teaches the means for the apparatus.

15. Claims 9 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over '569 and Stallings as applied above, and further in view of Ketcham US Patent No. 6,075,860 (hereinafter '860).

As per claim 9, '569 and Stallings teaches all the limitations of claim 1. Receiving a new user key set and automatically requesting access to the remote data network by the client device using a new user key set is already rejected in the arguments for claim 1. However, authenticating by the client device that the new user key set is received from a valid source is not taught in '569. Validating sources in which a user is connecting to is taught in '860 though, where a client device authenticates that the source in which it connects to is a valid source (col. 10 lines 10-37).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include validating a source in which a user is connecting to. One of ordinary

skill in the art would have been motivated to perform such an addition to create a mutual authentication channel in order for communication to be secure bidirectionally: "Furthermore, there exists a need for providing a method and system for establishing an encrypted authenticated wireless communication channel between an authorized user and a computer network."

Claim 12 is rejected using the same basis of arguments used to reject claim 9.

16. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over '569 and Stallings as applied above, and further in view of Walker et al. US Patent Application Publication No. 2003/0037250 (hereinafter '250).

As per claim 11, '569 and Stallings teaches all the limitations of claim 10, but does not teach an authentication database that associates a plurality of common key sets with a plurality of registration servers. However, '250 teaches a database associating keys with the respective servers (paragraph 17).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine an authentication system with an authentication database comprising of keys associated with their servers. One of ordinary skill in the art would have been motivated to perform such an addition to provide a secured access controller capable of communicating with a plurality of content servers: "It is a primary object of the present invention to provide a secured access controller for use in connection with a network capable of communicating with a plurality of content servers that store content objects

and a plurality of client processing systems capable of requesting access to the stored content objects" (paragraph 17).

17. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over '569 and Stallings as applied above, and further in view of Heller US Patent Application Publication No. 2002/0101857 (hereinafter '857).

As per claim 13, '857 teaches a user utilizing PPP for signaling with other devices. Paragraphs 19 and 20 summarize this. It is also discussed in paragraph 35 that this method is used to connect a user to a server.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the use of PPP for a client to signal systems in an authentication system and method. One of ordinary skill in the art would have been motivated to perform such an addition to improve the method and system for communicating information between a source and a destination using PPP: "Therefore, there is a general need in the art for an improved method and system for communicating information between a source and a destination using PPP. In particular, there is a need in the art for a method and system for communicating PPP packets between a source and a destination without the need for reconnection if the source is mobile" (paragraph 18).

As per claim 14, a client device is installed in a CPE comprising a DSL modem ('857 paragraph 14). Paragraph 27 of '857 teaches an IP router.

18. Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over '569 as applied above, and further in view of '860.

As per claim 16, '569 teaches all the limitations of claim 15. However, authenticating by the client device that the new user key set is received from a valid source is not taught in '569. Validating sources in which a user is connecting to is taught in '860 though, where a client device authenticates that the source in which it connects to is a valid source (col. 10 lines 10-37).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include validating a source in which a user is connecting to. One of ordinary skill in the art would have been motivated to perform such an addition to create a mutual authentication channel in order for communication to be secure bidirectionally: "Furthermore, there exists a need for providing a method and system for establishing an encrypted authenticated wireless communication channel between an authorized user and a computer network."

19. Claims 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over '569 as applied above, and further in view '857.

As per claim 17, '857 teaches a user utilizing PPP for signaling with other devices. Paragraphs 19 and 20 summarize this. It is also discussed in paragraph 35 that this method is used to connect a user to a server.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the use of PPP for a client to signal systems in an authentication system and method. One of ordinary skill in the art would have been motivated to

perform such an addition to improve the method and system for communicating information between a source and a destination using PPP: "Therefore, there is a general need in the art for an improved method and system for communicating information between a source and a destination using PPP. In particular, there is a need in the art for a method and system for communicating PPP packets between a source and a destination without the need for reconnection if the source is mobile" (paragraph 18).

As per claim 18, a client device is installed in a CPE comprising a DSL modem ('857 paragraph 14). Paragraph 27 of '857 teaches an IP router.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2134
07/14/06

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100